CLAIMS

1. A method for communication, comprising:

coupling a first port of a Layer-3 packet router to receive communication traffic from a network, the traffic comprising packets destined for a target address, which is accessible via a second port of the router;

at the router, diverting the packets that are destined for the target address to a traffic processor via a third port of the router;

processing the diverted packets at the traffic processor, and returning the processed packets to the router via the third port; and

at the router, conveying the processed packets from the third port to the second port for delivery to the target address.

2. The method according to claim 1, wherein diverting the packets comprises detecting an indication that at least some of the traffic destined for the target address is of malicious origin, and diverting the packets responsively to the indication.

3. The method according to claim 2, wherein processing the diverted packets comprises filtering the diverted packets in order to identify the packets of the malicious origin, and inhibiting delivery of the identified packets.

4. The method according to claim 1, wherein diverting the packets comprises sending a Border Gateway Protocol (BGP) announcement from the traffic processor to the router, instructing the router to divert the packets.

5. The method according to claim 4, wherein sending the BGP announcement comprises inserting at least one of a "no-advertise" and a "no-export" string in the BGP announcement.

6. The method according to claim 1, wherein diverting the packets comprises:

establishing a tunnel through the network from a peering router to the first port of the Layer-3 packet router;

configuring the Layer-3 packet router to forward the packets that it receives through the tunnel to the third port; and

instructing the peering router to forward the packets that are destined for the target address through the tunnel.

7. The method according to claim 6, wherein establishing the tunnel comprises establishing a plurality of tunnels from peering routers at an edge of an area of a network to the Layer-3 packet router within the area.

8. The method according to claim 1, wherein returning the processed packets comprises selecting, at the traffic processor, a path via the Layer-3 packet router to the target address, and directing the Layer-3 packet router to convey the processed packets to a next-hop router along the selected path.

9. The method according to claim 8, wherein selecting the path comprises identifying a plurality of paths, passing through respective next-hop routers to the target

address, and selecting one of the next-hop routers through which the processed packets are to be conveyed.

10. The method according to claim 9, wherein selecting the one of the next-hop routers comprises detecting, at the traffic processor, a change in the network between the second port of the router and the target address, and responsively to the change, selecting a different one of the next-hop routers through which to convey the processed packets to the target address.

11. The method according to claim 8, wherein selecting the path comprises receiving routing information at the traffic processor from the Layer-3 packet router, and identifying the path based on the routing information.

12. The method according to claim 11, wherein receiving the routing information comprises receiving announcements generated by routers in the network in accordance with an automatic routing protocol.

13. The method according to claim 12, wherein receiving the announcements comprises establishing at least one tunnel through the network between the traffic processor and the next-hop router, and receiving the announcements responsively to the at least one tunnel.

14. The method according to claim 11, wherein receiving the routing information comprises querying the Layer-3 packet router using a management protocol.

15. The method according to claim 8, wherein directing the router comprises establishing a tunnel through the network from the traffic processor via the router to the next-hop router, and passing the packets through the tunnel.

16. The method according to claim 1, wherein conveying the processed packets comprises programming the router with a forwarding rule with respect to the packets received by the router on the third port, so as to override a main routing table of the router, and forwarding the processed packets responsively to the forwarding rule.

17. The method according to claim 16, wherein programming the router comprises invoking policy-based routing (PBR).

18. The method according to claim 16, wherein programming the router comprises invoking filter-based forwarding (FBF).

19. The method according to claim 16, wherein programming the router comprises configuring the router to apply the forwarding rule responsively to a type of service (ToS) field in the processed packets, and wherein conveying the processed packets comprises setting a value of the ToS field in the packets so as to cause the forwarding rule to be invoked.

20. The method according to claim 1, wherein conveying the processed packets comprises adding a virtual private network (VPN) designation to the processed packets, and wherein conveying the processed packets comprises programming the router with a VPN routing table, and forwarding the processed packets responsively to the VPN routing table.

21. The method according to claim 20, wherein adding the VPN designation comprises adding a virtual local area network (VLAN) tag to the processed packets.

22. The method according to claim 21, wherein adding the VLAN tag comprises defining a plurality of VLANs corresponding to different routes to the target address, and wherein adding the VLAN tag comprises selecting one of the routes, and setting a value of the VLAN tag to designate the selected one of the routes.

23. A method for communication, comprising:

coupling one or more peering routers in an area of a network to receive communication traffic from outside the area, the traffic comprising packets destined for a target address;

forwarding the packets to the target address over one or more first routes via one or more internal routers within the area of the network;

establishing one or more tunnels through the network from the peering routers via one or more first ports of a diverting router within the area of the network to a second port of the diverting router;

coupling a traffic processor to the second port of the diverting router;

in response to a characteristic of the traffic, instructing the one or more peering routers to forward the packets that are destined for the target address through the one or more tunnels instead of over the first routes;

at the traffic processor, processing the packets that were forwarded through the tunnels via the diverting router; and

conveying at least some of the processed packets from the traffic processor to the target address.

24. The method according to claim 23, wherein instructing the one or more peering routers comprises detecting an indication that at least some of the traffic destined for the target address is of malicious origin, and instructing the one or more peering routers responsively to the indication.

25. The method according to claim 24, wherein processing the diverted packets comprises filtering the diverted packets in order to identify the packets of the malicious origin, and inhibiting delivery of the identified packets.

26. The method according to claim 23, wherein instructing the one or more peering routers comprises sending a Border Gateway Protocol (BGP) announcement from the traffic processor to the one or more peering routers.

27. The method according to claim 23, wherein instructing the one or more peering routers comprises sending an instruction to the one or more peering routers, without modifying routing tables of the internal routers.

28. The method according to claim 23, wherein the diverting router serves as one of the internal routers on at least one of the first routes.

29. The method according to claim 23, wherein conveying the at least some of the processed packets comprises conveying the at least some of the processed packets via the diverting router to the target address.

30. The method according to claim 23, wherein conveying the at least some of the processed packets comprises establishing a further tunnel between the traffic

processor and an edge router on a path to the target address, and conveying the at least some of the processed packets through the further tunnel.

31. A method for communication, comprising:

coupling a first port of a Layer-3 packet router to receive communication traffic from a network, the traffic comprising packets destined for a target address;

coupling a second port of the Layer-3 packet router to a subnet, through which the target address is accessible;

diverting the packets that are destined for the target address to a traffic processor on the subnet via a Layer-2 switch in the subnet;

processing the diverted packets at the traffic processor, and returning the processed packets to the Layer-2 switch; and

conveying the processed packets from the Layer-2 switch to the target address.

32. The method according to claim 31, wherein diverting the packets comprises detecting an indication that at least some of the traffic destined for the target address is of malicious origin, and diverting the packets responsively to the indication.

33. The method according to claim 32, wherein processing the diverted packets comprises filtering the diverted packets in order to identify the packets of the malicious origin, and inhibiting delivery of the identified packets.

34. The method according to claim 31, wherein the target address is in the subnet.

35. The method according to claim 31, wherein the target address is outside the subnet, and wherein conveying the processed packets comprises passing the processed packets from the Layer-2 switch to a further router in the subnet, and routing the processed packets from the further router to the target address.

36. Apparatus for communication, comprising:

a Layer-3 packet router, comprising at least first, second and third ports, wherein the first port is coupled to receive communication traffic from a network, the traffic comprising packets destined for a target address, which is accessible via a second port of the router; and

a traffic processor, which is coupled to the third port of the router, and is adapted to cause the router to divert the packets that are destined for the target address to the third port, and is further adapted to process the diverted packets and to return the processed packets to the router via the third port so as to cause the router to convey the processed packets from the third port to the second port for delivery to the target address.

37. The apparatus according to claim 36, wherein the traffic processor is adapted to cause the router to divert the packets responsively to an indication that at least some of the traffic destined for the target address is of malicious origin.

38. The apparatus according to claim 37, wherein the traffic processor is adapted to filter the diverted packets in order to identify the packets of the malicious origin, and to inhibit delivery of the identified packets.

39. The apparatus according to claim 36, wherein the traffic processor is adapted to send a Border Gateway Protocol (BGP) announcement to the router, instructing the router to divert the packets.

40. The apparatus according to claim 39 wherein the BGP announcement comprises at least one of a "no-advertise" and a "no-export" string.

41. The apparatus according to claim 36, and comprising a peering router, which is coupled by a tunnel through the network to the first port of the Layer-3 packet router,

wherein the traffic processor is adapted to instruct the peering router to forward the packets that are destined for the target address through the tunnel, and wherein the Layer-3 packet router is configured to forward the packets that it receives through the tunnel to the third port.

42. The apparatus according to claim 41, wherein the peering router is one of a plurality of peering routers at an edge of an area of a network, which are coupled by a respective plurality of tunnels to the Layer-3 packet router within the area.

43. The apparatus according to claim 36, wherein the traffic processor is adapted to select a path via the Layer-3 packet router to the target address, and to direct the Layer-3 packet router to convey the processed packets to a next-hop router along the selected path.

44. The apparatus according to claim 43, wherein the traffic processor is adapted to identify a plurality of paths, passing through respective next-hop routers to the

target address, and to select one of the next-hop routers through which the processed packets are to be conveyed.

45. The apparatus according to claim 44, wherein the traffic processor is adapted to detect a change in the network between the second port of the router and the target address, and responsively to the change, to select a different one of the next-hop routers through which to convey the processed packets to the target address.

46. The apparatus according to claim 43, wherein the traffic processor is coupled to receive routing information from the Layer-3 packet router, and is adapted to identify the path based on the routing information.

47. The apparatus according to claim 46, wherein the routing information received by the traffic processors comprises announcements generated by routers in the network in accordance with an automatic routing protocol.

48. The apparatus according to claim 47, wherein the traffic processor is coupled by at least one tunnel through the network to the next-hop router, and is adapted to receive the announcements responsively to the at least one tunnel.

49. The apparatus according to claim 46, wherein the traffic processor is adapted to receive the routing information by querying the Layer-3 packet router using a management protocol.

50. The apparatus according to claim 43, wherein the traffic processor is coupled to the next-hop router by a tunnel through the network via the router, and is adapted

to direct the Layer-3 packet router to convey the processed packets through the tunnel.

51. The apparatus according to claim 36, wherein the router is programmed to forward the processed packets in accordance with a forwarding rule, which overrides a main routing table of the router.

52. The apparatus according to claim 51, wherein the router is programmed using policy-based routing (PBR).

53. The apparatus according to claim 51, wherein the router is programmed using filter-based forwarding (FBF).

54. The apparatus according to claim 51, wherein the router is configured to apply the forwarding rule responsively to a type of service (ToS) field in the processed packets, and wherein the traffic processor is adapted to set a value of the ToS field in the processed packets so as to cause the forwarding rule to be invoked.

55. The apparatus according to claim 36, wherein the traffic processor is adapted to add a virtual private network (VPN) designation to the processed packets, and wherein the router is programmed with a VPN routing table, and forwards the processed packets responsively to the VPN designation in accordance with the VPN routing table.

56. The apparatus according to claim 55, wherein the VPN designation comprises a virtual local area network (VLAN) tag.

57. The apparatus according to claim 56, wherein the VLAN is one of a plurality of VLANs corresponding to different routes to the target address, and wherein the traffic processor is adapted to select one of the routes,

and to set a value of the VLAN tag to designate the selected one of the routes.

58. Apparatus for communication, comprising:

one or more peering routers in an area of a network, which are coupled to receive communication traffic from outside the area, the traffic comprising packets destined for a target address;

one or more internal routers within the area of the network, which are coupled to receive the packets from the one or more peering routers, and to forward the packets to the target address over one or more first routes;

a diverting router within the area of the network, the diverting router comprising one or more first ports and a second port, wherein the first ports are coupled to the peering routers by one or more tunnels through the network, and the diverting router is configured to pass the packets that it receives through the one or more tunnels to the second port;

a traffic processor, which is coupled to the second port of the diverting router, and which is adapted, in response to a characteristic of the traffic, to instruct the one or more peering routers to forward the packets that are destined for the target address through the one or more tunnels instead of over the first routes, and to process the packets that were forwarded through the tunnels via the diverting router, and to convey at least some of the processed packets to the target address.

59. The apparatus according to claim 58, wherein the traffic processor is adapted to instruct the one or more peering routers to forward the packets through the one or

more tunnels responsively to an indication that at least some of the traffic destined for the target address is of malicious origin.

60. The apparatus according to claim 59, wherein the traffic processor is adapted to filter the diverted packets in order to identify the packets of the malicious origin, and to inhibit delivery of the identified packets.

61. The apparatus according to claim 58, wherein the traffic processor is adapted to instruct the one or more peering routers to forward the packets through the one or more tunnels by sending a Border Gateway Protocol (BGP) announcement to the one or more peering routers.

62. The apparatus according to claim 58, wherein the traffic processor is adapted to instruct the one or more peering routers to forward the packets through the one or more tunnels without modifying routing tables of the internal routers.

63. The apparatus according to claim 58, wherein the diverting router is coupled to serve as one of the internal routers on at least one of the first routes.

64. The apparatus according to claim 58, wherein the traffic processor is adapted to convey the at least some of the processed packets via the diverting router to the target address.

65. The apparatus according to claim 58, wherein the traffic processor is adapted to convey the at least some of the processed packets through a further tunnel between the traffic processor and an edge router on a path to the target address.

66. Apparatus for communication, comprising:

a Layer-2 switch, located in a subnet through which a target address is accessible;

a Layer-3 packet router, comprising first and second ports, wherein the first port is coupled to receive communication traffic from a network, the traffic comprising packets destined for the target address, and the second port is coupled to the Layer-2 switch; and

a traffic processor, which is adapted to cause the Layer-3 packet router to divert the packets that are destined for the target address via the Layer-2 switch to the traffic processor, and which is further adapted to process the diverted packets and to return the processed packets to the Layer-2 switch so as to cause the Layer-2 switch to convey the processed packets to the target address.

67. The apparatus according to claim 66, wherein the traffic processor is adapted to instruct the Layer-3 packet router to divert the packets responsively to an indication that at least some of the traffic destined for the target address is of malicious origin.

68. The apparatus according to claim 67, wherein the traffic processor is adapted to filter the diverted packets in order to identify the packets of the malicious origin, and to inhibit delivery of the identified packets.

69. The apparatus according to claim 66, wherein the target address is in the subnet.

70. The apparatus according to claim 66, and comprising a further router in the subnet, wherein the target

address is outside the subnet, and wherein the Layer-2 switch is coupled to pass the processed packets to a further router in the subnet, and wherein the further router is adapted to route the processed packets to the target address.

71. A computer software product, for use by a computer in conjunction with a Layer-3 packet router that includes at least first, second and third ports, wherein the first port is coupled to receive communication traffic from a network, the traffic including packets destined for a target address, which is accessible via a second port of the router, and the computer is coupled to the third port, the product comprising:

a computer-readable medium in which program instructions are stored, which instructions, when read by the computer, cause the computer to instruct the router to divert the packets that are destined for the target address to the third port, and further cause the computer to process the diverted packets and to return the processed packets to the router via the third port so as to cause the router to convey the processed packets from the third port to the second port for delivery to the target address.